NUWC-NPT Technical Report 11,889
18 August 2008

Distributed Networked Force Value Proposition Implications for Distributed Networked System Concept Development

Robert C. Manke
Office of the Director of Undersea Warfare

NEWPORT

Naval Undersea Warfare Center Division
Newport, Rhode Island

Approved for public release; distribution is unlimited.

PREFACE

This report was prepared for the Director of Undersea Warfare at the Naval Undersea Warfare Center (NUWC) in support of the NUWC Undersea Distributed Networked Systems Initiative.

The technical reviewer for this report was Bruce I. Incze (Code 06).

The author is grateful for the comments provided by Raymond J. Christian and Frederick J. Pope.

Reviewed and Approved: 18 August 2008

Peter D. Herstein
Director, Undersea Warfare

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE (*DD-MM-YYYY*)	2. REPORT TYPE	3. DATES COVERED (*From – To*)
18-08-2008	Technical	

4. TITLE AND SUBTITLE

Distributed Networked Force Value Proposition Implications for Distributed Networked System Concept Development

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Robert C. Manke

5.d PROJECT NUMBER 7HQF180

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Undersea Warfare Center Division
1176 Howell Street
Newport, RI 02841-1708

8. PERFORMING ORGANIZATION REPORT NUMBER

TR 11,889

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Naval Undersea Warfare Center Division
1176 Howell Street
Newport, RI 02841-1708

10. SPONSORING/MONITOR'S ACRONYM

NUWC

11. SPONSORING/MONITORING REPORT NUMBER

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The U.S. Armed Services intend to conduct globally distributed and networked operations in support of the National Security Strategy. Instantiation of distributed networked operations (DNO) via a distributed networked force (DNF) is intended to provide influence over a greater geographic area while still providing the ability to rapidly concentrate combat power when required, thereby reducing the risk to warfighters and platforms. It is incumbent on the acquisition and technical communities to provide the globally distributed networked system (DNS) necessary to enable the DNF. It is important to understand the fundamental advantages—the value propositions—that must be inherent in a DNS concept to align it with the advantages of a DNF. This paper addresses (1) the distinction between a DNF and a DNS as applied to DNO, (2) the value propositions necessary for a DNS to enable the warfighting advantages of a DNF, and (3) the implication of a properly aligned set of DNS value propositions as a construct for a coevolution of force-multiplying DNS technology and operational concepts and the associated operational experimentation hypotheses development. This paper will assist the practitioner developing and experimenting with DNS concepts to establish a link to the value of a DNF.

15. SUBJECT TERMS

Distributed Networked Operations DNO	Distributed Networked Force DNF	Distributed Networked System DNS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Robert C. Manke
(U)	(U)	(U)	SAR	27	19b. TELEPHONE NUMBER (*Include area code*) (401) 832-8252

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF ABBREVIATIONS AND ACRONYMS

AAW	Anti-air warfare
AOU	Area of uncertainty
ASW	Antisubmarine warfare
C^2	Command and control
CONOPS	Concept of operations
CSG	Carrier strike group
DMER5	Deployment, management, exploitation, redeployment, refueling, repositioning, replacement, recovery
DNF	Distributed networked forces
DNO	Distributed networked operations
DNS	Distributed networked system
DOD	Department of Defense
DOTMLPF	Doctrine, organization, training, materiel, leadership and education, personnel, facilities
ESG	Expeditionary strike group
EW	Electronic warfare
ISR	Intelligence, surveillance, and reconnaissance
METOC	Meteorological and oceanographic
NOC	Naval Operations Concept
ROE	Rules of engagement
RSTA	Reconnaissance, surveillance, and target acquisition
SME	Subject matter experts
TRL	Technology readiness level
TTP	Tactics, techniques, and procedures
UAV	Unmanned air vehicle
WMD	Weapon of mass destruction

DISTRIBUTED NETWORKED FORCE VALUE PROPOSITION IMPLICATIONS FOR DISTRIBUTED NETWORKED SYSTEM CONCEPT DEVELOPMENT

1. INTRODUCTION

The U.S. Armed Services intend to conduct globally distributed and networked operations in support of the National Security Strategy.[1] Instantiation of distributed networked operations (DNO) via a distributed networked force (DNF) is intended to provide influence over a greater geographic area while still providing the ability to rapidly concentrate combat power when required, thereby reducing the risk to warfighters and platforms. It is incumbent on the acquisition and technical communities to provide the globally distributed networked system (DNS) necessary to enable the DNF. It is important to understand the fundamental advantages—that is, the value propositions—that must be inherent in a DNS concept to align it with the advantages of a DNF.

The ability to operate a global distribution of forces is based on the premise that the minimum number of system nodes needed to generate the desired effect is available. There are various indications that this is not the case across the Armed Services, whether the nodes are soldiers or ships. One example is the method being employed by the U.S. Navy to increase maritime nodes—the Global Maritime Partnerships Initiative ("1,000-Ship Navy").[2] Another method (these methods are not mutually exclusive) is the addition of unmanned devices, unmanned vehicles, and smaller manned platforms. The reality, at least in the maritime domain, is that DNF capabilities are currently limited by the number of DNS nodes and the connectivity between the nodes. Thus, the realities of acceptable warfighting risks and affordable capital platform force levels drive the need for force-multiplication capabilities. The combatant commander's demand signal might challenge the acquisition and technical communities to develop viable force-multiplying maritime DNS concepts.

This paper addresses (1) the distinction between a DNF and a DNS as applied to DNO, (2) the fundamental advantages or value propositions necessary for a DNS to enable the warfighting advantages of a DNF, and (3) the implication of a properly aligned set of DNS value propositions as a construct for a coevolution of force-multiplying DNS technology and operational concepts and the associated operational experimentation hypotheses development. Examples are provided. The intent of this paper is to assist the practitioner who is developing and experimenting with DNS concepts to establish a link to the value of a DNF.

2. DISTRIBUTED NETWORKED OPERATIONS AND DISTRIBUTED NETWORKED FORCES

2.1 BACKGROUND

Throughout history military strategists and tacticians have studied the pros and cons of concentrating or distributing armed forces. Both methods have been employed with success and failure. The success or failure of a strategy or tactic hinges on its alignment with the nature of the opposition forces, its alignment with the posture of own forces, and its alignment for countering the opposition's strategies and tactics.

U.S. Armed Forces policy and concept documents have increasingly reflected the desire to operate in a posture that is distributed globally or regionally, yet is responsive and adaptive enough to bring combat power to bear against an adversary. For example, in 2005, General M. W. Hagee, Commandant of the Marine Corps, signed "A Concept for Distributed Operations" that defined distributed operations as

> … an operating approach that will create an advantage over an adversary through the deliberate use of separation and coordinated, interdependent, tactical actions enabled by increased access to functional support, as well as by enhanced combat capabilities at the small-unit level. The essence of this concept lies in the capacity for coordinated action by dispersed units, throughout the breadth and depth of the battlespace, ordered and connected within an operational design focused on a common aim.[3]

The U.S. Navy has reemphasized its intent to operate in a distributed manner in the Naval Operations Concept (NOC). Regarding methods of organizing, training, equipping, deploying, or operating, the NOC states:

- Globally Networked Operations – Establishing a scalable open access/open architecture information system to enhance organizational flexibility and global awareness. Our system must facilitate the rapid information sharing required to expeditiously task-organize and employ Navy and Marine Corps forces from worldwide locations, while appropriately safeguarding sensitive or classified information.

- Distributed Operations – Increasing our ability for independent, unified action by geographically separated, yet globally, regionally, or tactically integrated, networked forces. Decentralized action will permit wider, more diverse application of naval power and influence. The connectivity afforded by distributed operations permits rapid reaggregation or reinforcement where military power projection must be quickly applied. It also places a premium on situational awareness and judgment of junior leaders, thereby necessitating enhancements to professional development.[4]

"Distributed networked operations" in various forms are part of the current military lexicon. Military risk management is critical to the current emphasis in DNO.

2.2 RATIONALE BEHIND DNO AND ASSOCIATED DNF

The rationale for when to distribute or concentrate forces is based on assessment of the risk associated with achieving various operational objectives. The distribution or concentration of forces requires varying degrees of communication to be effective. The advances in information technologies enable a degree of interaction beyond simple communications. The potential of this higher level networking enables distributed force attributes not feasible in the past. This section addresses the rationale behind distributed and networked forces.

2.1.1 Distributed Forces

Combat power is distributed across geographically spaced forces for various *strategic* and *tactical* reasons that are dependent on the nature of the adversary and own force posture. Strategically, the reason for distribution differs for conventional campaigns, or regular warfare, and irregular warfare.*

From a conventional campaign perspective, one *strategically* distributes forces to confuse the adversary about your intended objective(s). The objective of a direct concentrated thrust may be readily apparent to an adversary, who is thus allowed time to strengthen defenses. The use of distributed forces, if identified by the adversary, could be interpreted as a drive toward numerous objectives and thus could cause the adversary to pause. The combat power from the distributed forces can be directed to single or numerous objectives. Distributed forces can distract the adversary's mind and force. Care must be taken to maintain distribution distances that are within the ability of own forces to conduct combined action, i.e., distances that are within the physical reach of own force power and logistics and that are within any communications limits.[7]

In the case of irregular warfare and its manifestation through guerrilla warfare or terrorism, distribution is a preferred strategy of the adversary. Force distribution is a means of survival for the adversary who wants to avoid engaging a major force concentration and thus live to fight another day. Distributing forces within the local environment provides a degree of concealment. The adversary wants to use asymmetric means to strike at times of his choosing, create damage, and fold back into the environment. This strategy applies to either land or maritime warfare.[8,9,10]

Concentration of own forces against distributed irregular forces can be advantageous to the adversary. It is conceivably easier for the adversary to find the concentrated force and harder for

---

*A conventional campaign refers to a conflict occurring between recognized nation-states and the use of regular forces (state-sponsored armed forces or other internal forces). A conventional campaign may be related to total war or limited war. In total war, the survival of either side is at stake. In limited war, (1) the survival of either side is not at stake, (2) the objective of the conflict may have nothing to do with occupying territory but may be based on establishing conditions for political settlement, (3) the objective is to avoid escalation to the brink of nuclear power use, (4) the objective is to minimize damage to the civilian population and infrastructure, and (5) the objective is to minimize perception of U.S. hegemony and imperialistic expansion.[5]

Irregular warfare refers to a conflict "among state and non-state actors for legitimacy and influence over the relevant population(s). [It] favors indirect and asymmetric approaches, though it may employ the full range of military and other capabilities, in order to erode an adversary's power, influence, and will."[6] Irregular armed forces are " armed individuals or groups who are not members of the regular forces, police, or other internal security forces."[6]

the concentrated force to find a distributed adversary. Concentrated force may be meaningless if the adversary is not encountered. Own forces want to use distribution to cast the widest possible net over an area.[7] The alternative is a defensive stance. Again, own force distribution must be within the physical and communications limits.

At the *tactical* level, a concentration or a distribution of own forces is based on the defensive capability or vulnerability of the force. If the adversary has the ability to reach out and strike with a blow sufficient to eliminate the massed combat power, then one wants to distribute own forces. This distribution serves to complicate the adversary's targeting ability. Operating within the physical limits is dependent on the aggregate nature of the defensive posture[9] (e.g., the antisubmarine warfare (ASW) posture and anti-air warfare (AAW) posture of strike groups may require differing distribution arrangements of escort ships, which poses a command dilemma). Note the difference in this discussion between a more deliberate distribution of forces and a more reactive dispersal under duress.

In the foreseeable future, the United States will have a superior naval force as compared with any other nation.* Any adversary's inferior navy would most likely employ his naval forces for anti-access/area denial purposes. Military theory identifies strategies that an inferior navy would employ in a conflict against superior forces: (1) maintaining the force, (2) active defense, and (3) local superiority while exploiting various asymmetries.[5] All three strategic elements require the adversary to distribute forces. The resultant implications should lead the United States towards a distributed force posture.

The superior navy, anticipating the inferior navy's strategy, would employ certain access strategies as a counter. Strategic elements for the superior navy include (1) minimizing vulnerabilities to asymmetric warfare, (2) prevention of attack through asymmetrical strengths, and (3) deterrence.[5] The superior force could minimize vulnerabilities by distributing centers of gravity within defensive capability limits. The force would attempt to prevent attacks by denying the adversary any sanctuaries from which to stage attacks. A distributed force may also be required to generate the necessary geographic footprint to identify and eliminate sanctuaries of the adversary's asymmetric and concealed force. If the superior maritime forces are located close to an adversary's shore, where the adversary can employ "joint" capabilities, it may be necessary to distribute forces for defensive purposes.

2.1.2 Force Networking

It was noted above that a key aspect of distributed operations must be working within the limits of own forces' cohesive combat power. This means reconciling the distribution of forces with the physical reach and timeliness of sense, control, and respond capabilities. Communications have always been a limiting factor in the distribution of forces or in the distribution of the sense, control, and respond functions. This is true whether communications

---

*The traditional definition of superior force is based on the tendency to, in the words of General Rupert Smith, "measure potential military force by counting the men, ships, tanks and aircraft of all sides and … compare one inventory with another, measuring the balance of power accordingly." He cautions that "comparing inventories can lead to dangerously simplistic judgments at the outset."[11] In this report, "superior naval force" refers to the warfighting force composed of the combined capability and capacity of the naval forces.

are between warfighters, platforms, or systems. Networking is a key enabler in minimizing this limitation across geographically and hierarchically distributed elements. From a warfighting perspective, this is first about communication links, but, with the advances in technology, it is quickly about the *interactions and relationships* of warfighters, platforms, and systems enabled by the communication links.

2.1.3 Distributed Networked Force Value Proposition

Military theory suggests that there are strategic and tactical benefits to the distribution of military force that are appropriate to the nature of the adversary the United States may encounter. The advances in information technologies and the ability to network provide significant improvement against the limitations imposed on distributed forces in the past. Together, there is a synergy that has the potential to greatly enhance warfighting capability. This synergy is such that a properly structured and outfitted distributed networked force provides the following value propositions to the nation:

- Distributed forces distribute warfighting risk.
- Distributed networked forces provide agility and thus a greater number of options for the commanding officer.
  - Distributed forces influence a greater geographic area.
  - Distributed networked forces enable timely and adaptive concentration of combat power when required for strategic, operational, and tactical advantage.

From a maritime perspective, these values apply at various levels of force hierarchy whether the distribution is at the task group level or at the cross-maritime service and international coalition level stated in the newest U.S. maritime strategy.[12] This is the basis for the requirement in the NOC for globally distributed and networked operations.

3. DISTRIBUTED NETWORKED SYSTEM (DNS) WARFIGHTING VALUE

3.1 DEFINITION OF DNS

The U.S. military services have been transforming their forces to support geographically and hierarchically distributed operations. DoD Joint Publication 1-02 defines military force as "an aggregation of military personnel, weapon systems, equipment, and necessary support, or combination thereof."[6] Implicit in this definition is the assumption that the force comprises a system of elements that must work together in harmony. These elements are doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF).[6]

It is important to understand the characteristics of the DOTMLPF element characteristics required to enable a distributed networked force. It is easy to think of a distributed networked "system" as the technology elements of, or a portion of the "M" in, DOTMLPF, but the application of operational art* to a properly trained and ready force using the technology elements constitutes real operational capability. This means that a DNS has hierarchical definitions similar to distributed networked forces. (From the above, the distributed networked force can be defined from the platoon or task group up to the international coalition level.)

The greater part of this paper will address the DNS construct at the technical and operational capability level in the hierarchy. At this level, Christian defines a DNS as "…a large group of interacting, independent, and diverse elements and connections that, based on system-induced information transactions, respond with or without central direction in varied, yet coherent, aggregate behavior appropriate to the USW conditions."[14] Put more simply, a DNS is *a complex interacting group of warfighters, platforms, devices, and connections that, based on information networking, respond to various degrees of control and achieve the commander's intent in a coherent, aggregate manner.*

It is important to understand the functions performed by the DNS that will enable the DNF. The DNS functions are defined as follows:

- Sensing – collecting observations of objects and the environment within the area of interest.

- Transport – providing mobility for system elements that may not have their own locomotion or for elements more effectively moved by other elements.

- Netting – creating the means for information (data and control) transfer between elements of the system.

- Information Fusion and Pattern Recognition – sharing information among the system elements for the purposes of receiving observations from sensors, composing

---

*Operational art is a translation or planning process that links ends, ways, and means in the application of military force.[13] In other words, how does one use particular aspects of combat power to achieve particular effects and objectives?

informational representations of the battlespace, and determining important patterns within the representations.

- Interpretation, Cognition, and Decision – consuming information, deliberating and converting deliberation into decisions across the entire command structure.

- Influence – acting to change physical, informational or logical states in the battlespace.[15]

3.2 DNS VALUE PROPOSITIONS

If the DNF is going to distribute warfighting risk, provide greater options for the commanding officer, influence a greater geographic area, enable a rapid concentration of combat power, and deny the adversary the ability to effectively concentrate combat power, the DNS functions must be turned into system elements and provide the following value or advantages:

- Creation of pervasive, persistent sensing sufficient for sustained awareness.

- Augmentation, then replacement of, force-on-force with distributed force and massed effects.

  - Extended capability reach via combat power distribution across manned and unmanned platforms.

  - Creation of options for risk tolerance and robustness.

  - Sufficient numbers and speed for rapid concentration of mass as needed on demand.

- Creation of a distributed networked force to share awareness and to conduct distributed operations enabling

  - Force dispersal, hiding, and greater standoff range;

  - Surprise, preemptive, retaliatory, containment attack on the adversary from unpredictable sources;

  - More rapid distributed employment decisions;

  - Greater economy of force; and

  - Greater actual firepower from joint and allied forces.

- Creation and/or exploitation of the adversary's tactical instability* through disruption, desynchronization, and destruction of
  - Key high-threat, low-density forces;
  - Reconnaissance, surveillance, and target acquisition (RSTA) systems, and
  - Command and control.[14]

These advantages, which are thus desired attributes, should seem familiar. The warfighter is always looking to improve capabilities along these lines. It is important that realistic quantification of these attributes instantiated within a DNS be consistent with the spatial and temporal dimensions associated with the adversary's capabilities applied to potential conflicts (i.e., a conventional campaign, a war on terror/irregular warfare, and homeland defense).[†] These broad DNS value propositions are applicable across all warfighting domains (land, maritime, air, and space) within the DNF context.

As the nature of the threat evolves over time, the spatial and temporal dimensions of potential conflicts are likely to change. One major driver behind this change will be the continued exploitation of new technologies with the potential to dramatically change the battlefield. This will change the manner in which the United States projects power and the manner in which adversaries will conduct anti-access/area denial operations.

Two major technology drivers of the probable evolution of the DNS are unmanned vehicles/offboard devices and the information technology necessary to support more robust command and control. It is likely that the evolution of warfare systems will progress in the manner shown in figure 1.

---

*Based on the work of CAPT (Ret.) Wayne P. Hughes, Jr., Christian writes: "The concept of tactical stability compares the combat power of a force to its survivability … . In a tactically stable force, combat power and survivability are approximately equal. If combat power is greater than survivability, a force becomes tactically unstable because it grows risk-averse. A force whose survivability grows at a rate greater than its combat power is of little value because it cannot do much more than survive."[14]

[†]A conventional campaign, a war on terror/irregular warfare, and homeland defense are the three conflict domains identified in the 2006 Quadrennial Defense Review.[16]

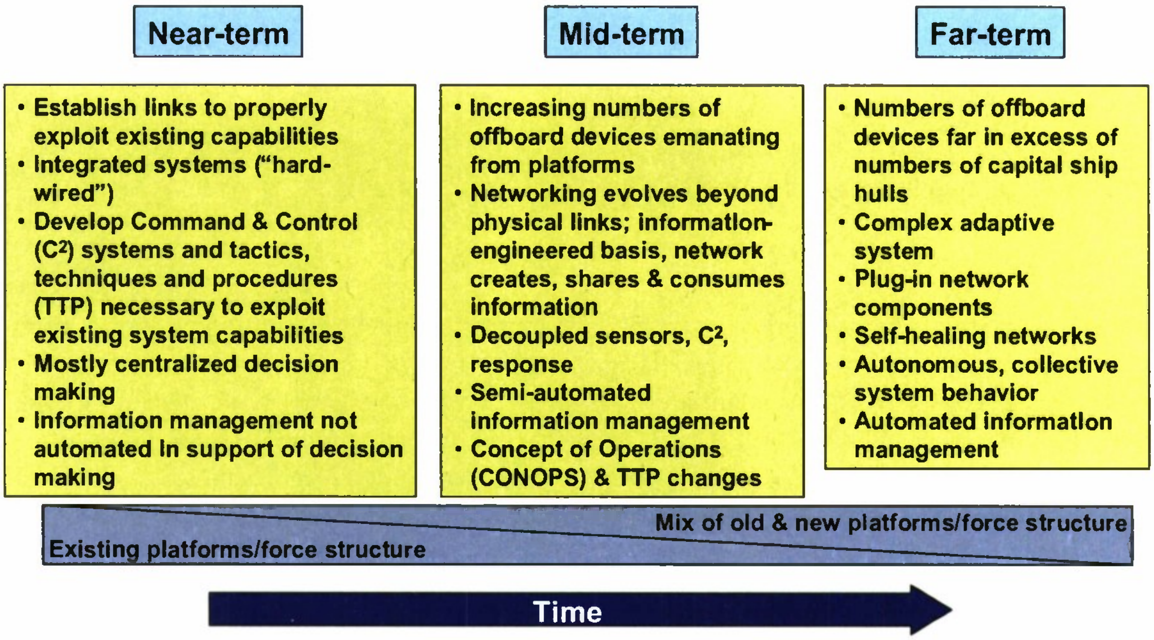

Figure 1. Possible Warfare System Evolution

It is thought by some that this progression to a DNS composed of greater numbers of distributed and networked unmanned nodes is inevitable if the desired value propositions are to be realized against future adversaries.*

It is important that operational concepts and capabilities be explored across the construct of evolving warfare systems to determine to what extent the value propositions are operationally realizable and affordable.

*Christian[14] provides examples of the fundamental paradigm shifts envisioned as enabled by this warfare system evolution for the DNS functions, from sensing to influence.

4. EXAMPLES OF DNS VALUE PROPOSITIONS APPLIED TO THE MARITIME DOMAIN

Application of the DNS value propositions to viable operational concepts must be based on the operational dimensions of the potential theaters of interest and on the ability to scale capabilities to the risk posed by the adversary. This means the DNS concept developers (engineers and end users) have two trade spaces in which to operate:

- Operational capability trade space:
  - Force (capability and capacity), space, and time.
  - DMER5.*
- Technical capability trade space:
  - Functions (e.g., sense and influence), speed, mobility, and stealth.
  - Technology readiness level (TRL), manufacturability, and cost.

Examples of the DNS contributions to the DNF value propositions are provided in this section as an aid to the concept developer. A series of hypothetical maritime examples of force-multiplying, DNS concepts are provided to explore the operational and technical trade space. Four examples are related to ASW, and the fifth example is related to intelligence, surveillance, and reconnaissance (ISR). Exploration of the actual technologies and resultant DMER5 are left to the concept developer and experimenter.

4.1 ASW BARRIER

ASW barriers are established to deny passage to an adversary's submarine, thus restricting its movement, or to allow passage of the submarine and provide command authority awareness of the submarine's movement. The former type of barrier is achieved through denial, diversion, or deterrence. The latter type of barrier is achieved with a trip wire and may provide a count of egressing platforms, an indication of maneuver direction, and, perhaps, continued awareness of the platform location based on subsequent tracking of the platform.

An ASW barrier can be implemented by various generic options, such as described in the examples below:

- Single ASW platform – conducts search, track, and kill as required.
- Single ASW search platform with single ASW pouncer (track or kill) platform.

---

*DMER5 refers to the employment factors that must exist with any capability to render it operational: deployment, management, exploitation, redeployment, refueling, repositioning, replacement, and recovery.

- Multiple fixed sensors or unmanned search platforms with a single manned ASW pouncer.

- Multiple fixed sensors or unmanned search platforms with multiple pouncer platforms and devices.

The use of multiple search and pouncer platforms or devices may be required if the operational scenario includes the possibility of multiple submarines transiting from a port or through a choke point.

Geography determines where barriers should be positioned. The available operational capability may determine the ASW barrier length. For example, a port barrier composed of manned ASW platforms may need to be positioned farther at sea than a barrier of unmanned devices. Because of risk considerations, a barrier positioned farther at sea most likely correlates to a longer barrier length and perhaps the need for more platforms.

Consider a port egress barrier of 60 nmi. Assume the acoustic conditions are such that two manned platforms with their organic capabilities are required to provide awareness of the submarine transit with a probability of 90%. The concept of operations (CONOPS) or tactical objective might call for the acquiring ASW platform to follow the transiter. The result would be that half of the barrier would be left open to other transiters.

Another CONOPS might call for the notification of an additional ASW platform, a pouncer, to reacquire, follow, and/or kill the transiter depending on the rules of engagement (ROE). Based on the kinematics of the scenario, the pouncer would need to be positioned farther at sea and thus would need to form a second barrier of greater than 60 nmi. This CONOPS would require 3 manned ASW platforms for this one port egress barrier example. If the barrier is against a formidable anti-access/area denial adversary the manned ASW platforms may need to be submarines. Given other theater requirements and the multi-mission nature of the platform, resource allocation tradeoffs will be required.

Complementary force, space, and time trades are possible with the use of unmanned devices (fixed devices or mobile vehicles). If unmanned devices can be employed closer to the adversary's shore, the search barrier might be reduced to 30 nmi. If each unmanned node has a 3-nmi capability, 10 nodes would be required to replace the two manned ASW search platforms. The unmanned sensing barrier can potentially provide information sufficient for the targeting of an ASW standoff weapon from the manned ASW pouncer. The force-multiplication aspects of this concept are apparent. A more forward-located sensing barrier would provide additional time for the pouncer to react. Greater coverage options may not be possible without a DNS.

This is a simple scenario, but it illustrates how a DNS with an increased ratio of unmanned nodes to manned platforms provides values stated in section 3.2.

- *Creation of pervasive, persistent sensing sufficient for sustained awareness.* If the need for persistence requires a redundancy of fixed devices or mobile platforms that increases the node count, trades are required among the DMER5 elements. If the unmanned concept is achievable, persistent sensing may also be achievable, given that the manned platform may be reassigned to higher priority tasking.

- *Extended capability reach via combat power distribution across manned and unmanned platforms.* The force multiplication and extended reach advantages are evident.

- *Creation of options for risk tolerance and robustness.* The above construct allows the possibility of close-in sensing capability with greater standoff attack capability. The risk is shifted from a manned platform to an expendable device.

- *Creation of a distributed networked force to share awareness and to conduct distributed operations.* The above construct allows distribution of the sensing and influencing actions. If a single pouncer can provide the standoff attack capability for the full barrier, the construct provides an economy of force.

There are considerable operational and technical challenges associated with realizing this distributed construct. A coevolution of technology and operational concepts will be required to determine the required numbered of achievable devices, the full range of DMER5 elements, the expense of and countermeasures to the unmanned devices, the affordability, and ultimately the risk to the warfighter and to the operational objectives. If this construct is realizable, it enhances the DNS value proposition.

4.2 ASW AREA CLEARANCE AND DENIAL

A more complex ASW scenario, which is arguably more challenging, is the monitoring of a large sea base for adversary submarine activity. This initially entails searching the entire sea base for a submarine presence. A searched and cleared area then needs to be monitored against submarine incursion. If mobile search sensors are used for the initial clearance or subsequent denial, the need to repeat the area search must be included because the probability of a submarine being present will increase as the area searched goes "cold." The monitoring may be provided by an ASW barrier around the sea base, an area monitoring system within the sea base, or both, depending on the degree of certainty required. The persistence requirement for monitoring will be variable, depending on the nature of the sea base—carrier strike group (CSG), expeditionary strike group (ESG), or logistic ship(s).

The tradeoffs between force, space, and time are limited with the current Fleet force level. Figure 2 illustrates how the current reduction in force level impacts the composition of a carrier strike group. The picture on the left is the USS Kittyhawk Battle Group in 1993.

Figure 2. Changed Battle Group Composition

The picture on the right is the USS Nimitz Battle Group in 2005. Current battle groups place greater defensive demands on fewer escort platforms.

Because the number of combatants will not dramatically increase over the next decade, it is imperative that a force-multiplication capability be developed. Augmentation of the force with unmanned devices will allow a greater space to be covered. Coverage of a greater space will provide the command authority more time to react to an emergent threat and more space in which to maneuver. More DNS nodes will allow the force, space, and time trades necessary to reduce risk to the battle group.

There are various generic force-multiplication options, such as those listed below:

- Search the area with the manned ASW platform(s) and leave behind an unmanned sensor field (fixed, floating, mobile) to monitor the area.

- Establish an unmanned trip wire sensor field to monitor the sea base perimeter, and search within the area once with the manned ASW platform(s).

- Utilize a combination of manned ASW platform(s) and a distributed field, where the field is used to augment the manned platform(s).

The first two options for monitoring the field allow the use of the manned ASW platform as a pouncer if the submarine is found within the sea base. This use may be direct or standoff in nature. It could free the platform to perform additional missions within the sea base, such as AAW, or to search new sea base locations. The third option might require the manned platform to have ASW standoff weapon capability in order for it to maintain its search station.

The persistence requirement for any unmanned sensing devices is highly dependent on the sea base CONOPS:

- Sea base location remains geographically constant. If a highly effective trip wire can be developed around the sea base, it needs to be enduring to maintain area denial. If the trip wire is highly effective, only limited-duration area clearance devices will be required. Longer-duration devices will be required if the trip wire effectiveness is such that a secondary layer is required.

- Sea base changes location. If the sea base location changes on a periodic basis, the duration of the area clearance devices must extend through that time period. After the initial area clearance, they become area denial devices.

A number of concepts exist for mobile, floating, and fixed sensor fields using traditional and nontraditional means to detect and track a submarine. Any of these concepts will result in a DNS with an increased ratio of unmanned nodes to manned platforms. The advantages of these concepts, if realizable, enhance the DNS value propositions stated in section 3.2 as explained below:

- *Creation of pervasive, persistent sensing sufficient for sustained awareness.* As in the barrier scenarios, the need for persistence in clearing and monitoring a sea base may require a redundancy of unmanned sensors or vehicles. The unmanned nodes provide a level of pervasiveness and persistence not achievable with the available manned platforms. This may be due to the realities of force levels or the need to position the platforms for AAW optimization at the expense of ASW optimization.

- *Extended capability reach via combat power distribution across manned and unmanned platforms.* The force multiplication and extended reach advantages are evident.

- *Creation of options for risk tolerance and robustness.* Given the force level realities, these concepts provide greater ASW robustness and thus reduced risk to the sea base. Greater ASW robustness, especially in concert with ASW standoff weapons, frees platforms to concentrate on other missions such as AAW.

- *Creation of a distributed networked force to share awareness and to conduct distributed operations.* These concepts allow distribution of the sensing and influencing actions. Augmenting manned platforms with standoff attack capability with mobile, floating, or fixed ASW sensor fields constitutes an economy of force.

- *Creation and/or explotation of the adversary's tactical instability through disruption, desynchronization, and destruction.* The use of persistent sensing and monitoring fields creates a greater vulnerability for the adversary, which alters his tactical stability.

The complexity level for ASW increases greatly at the theater level. Consider a scenario with the need for ASW protection of two to three carriers or amphibious vessels and their logistic sea base, all geographically dispersed. The scenario could become even more complex if the strike groups need to fight their way into position instead of having the opportunity to establish a sea base before the outbreak of hostilities. Demands on ASW assets could be further complicated if the adversary's submarines create a presence far out-of-area at our forward bases or off allied coasts, thereby freezing or delaying ASW assets from getting to the theater. A higher degree of ASW robustness, enabled by an enhanced DNS, is required to reduce the risk posed by these scenarios.

As in the previous example, this and the subsequent examples will require a coevolution of technology and operational concepts to determine whether the concepts are realizable.

4.3 ASW FORCE EMPLOYMENT—REACHBACK

Force multiplication can take many forms. One form is adding unmanned assets to the theater, as described in section 4.2. Another form is using out-of-theater assets to augment the capabilities of in-theater assets, thereby increasing their effectiveness and efficiency. One example is reachback to operate forward-deployed unmanned systems. Another example is reachback to subject matter experts (SME). A specifically maritime example is reachback for assistance in the detection and classification of adversary submarines.

This assistance could take different forms, progressing from assistance to a single platform to assistance across a theater of operations. In the former case, data collected by the platform's organic sensors could be forwarded to an SME located on another platform or ashore. The more experienced SME may be able to more rapidly confirm or discount a preliminary finding. The SME could recommend searching for other target-specific discriminators that would aid in the detection and classification process. If this concept could be realized in near-real time, the time required to investigate targets of interest and identify false targets could be reduced.

At the operational level, the collective ASW data from the theater might be forwarded to an SME for assessment. SMEs may be experts in particular sensing domains—e.g., acoustic or visual—or in operations research—e.g., multiplatform search effectiveness. Further, SMEs could have access to all-source information, which can be correlated with the platform data. Maritime domain awareness data could be correlated so as to reduce the number of false targets. SMEs would have access to better meteorological and oceanographic (METOC) data and therefore would have more accurate prediction capabilities. This is not to say that reachback should replace in-theater capabilities, but there may be advantages associated with different looks at the data and more collaborative planning and decision making.

The advantages of these concepts, if realizable, enhance this DNS value proposition from section 3.2:

- *Creation of a distributed networked force to share awareness and to conduct distributed operations.* The concepts discussed above enhance the development of a more timely and accurate ASW situational awareness. The result is to reduce the time necessary to prosecute a target of interest and thereby reduce the probability of a missed submarine transiter.

Trade space analysis is required to determine under what loading conditions these concepts become advantageous. There may be little to no value in reachback to the sensor operator if the conditions are such that there are few contacts at any given time. The advantage would appear when the contact load becomes heavy enough that the operator does not have the opportunity to investigate all contacts and thus may potentially miss the target of interest or a second target of interest that may be present.

A similar trade space analysis is required at the operational level. There may be little value to reachback if the number of ASW nodes is low. As the number of nodes increases, a corresponding increase in the loading from false contacts would be expected, and a reachback capability is more likely to be an advantage. Further, it is conceivable that, as the number of DNS nodes increases, the false contact problem is simplified because there are more accurate contact data.

4.4 ASW FORCE EMPLOYMENT—REPOSITIONING

A key premise of distributed networked forces is the use of information to make forces more effective through better employment. This is especially important if the numbers and capabilities of tactical platforms are limited in particular tactical situations.

Consider the ASW barrier examples from section 4.1. A tactical situation may arise in which the adversary decides to flood a particular portion of the barrier to improve the number of submarines that successfully penetrate. This may be to overload track or kill assets depending on the ROE. It may be an attempt to allow a higher value unit to egress while ASW forces are occupied with a lesser value unit.

The DNS barrier concepts described in 4.1 enhance defense capabilities against such tactics. Employment of unmanned devices closer to port can provide more time to recognize the emerging situation, make decisions, and begin to move tactical assets into position as necessary.

The advantages of options for repositioning forces when employing ASW barriers, if realizable, enhance the DNS value propositions stated in section 3.2 as explained below:

- *Creation of pervasive, persistent sensing sufficient for sustained awareness.* The use of unmanned sensing devices creates a persistent awareness of activity in the barrier. A manned platform acting as a sensing and/or response platform could conceivably be pulled off the barrier while tracking the first submarine transiter. If this occurs, command authority can still be alerted to the egress of other, perhaps higher value, submarines.

- *More rapid distributed employment decisions.* The more timely awareness of multiple submarine egress allows better decisions to be made as to which, if any, submarine to follow. If multiple pouncers are available, they can be positioned to pick up the transiters more effectively. If additional pouncers need to be brought to the barrier, they may be vectored more effectively and given the distinguishing characteristics of particular hulls to aid in target reacquisition.

- *Greater economy of force.* Depending on the tactical situation, numerous manned platforms do not need to be stationed waiting to pounce. One pouncer will suffice, with other platforms assigned to pouncer status if required by the situation.

4.5 ISR FORCE DISPERSAL

ISR exploitation of various discriminators increasingly requires proximity or line-of-sight sensing. This is true for a broad range of ISR, including weapons of mass destruction (WMD) monitoring, electronic warfare (EW), underground facility detection and monitoring, and monitoring of high-profile person movement. This is especially true when gathering evidence sufficient for proof in the World Court.

ISR against WMD, EW, underground, and personnel targets presents interesting challenges. Line-of-sight requires accurate knowledge of where to be positioned. Line-of-sight locations may necessitate covert or clandestine capabilities. Proximity requirements will most likely require covert or clandestine capabilities. Both cases may require positioning closer to an adversary than a manned platform could prudently operate. If the basic operational scenario arises from the Global War on Terror, the physical harm to manned platforms may be deemed less of a risk than the potential political liabilities.

These challenges lead to the need for force multiplication to achieve the required operational capability at or below a tolerable level of risk. Force multiplication extends the area of regard of a manned platform. In one case, the footprint may be distributed over an area to determine the optimal ISR locations. If multiple locations exist, there may be the need to position multiple sensors. In other cases, the extended footprint may simply consist of a single sensor strategically located.

Exploitation of a discriminator may lead to the need for a time-critical response—either preemptive or retaliatory. This is similar to the evolution of capabilities seen in UAVs, which have progressed from sensing devices to response devices. If this is a possibility, the sensor, or sensor field, may have to be designed and employed to support targeting. For other types of sensors or sensor fields, there is a tradeoff between the search/monitor sensor generated area of uncertainty (AOU) and the reacquisition sensor field of regard on the response/influence device. There are also the tradeoffs between the search/monitor sensor size, capability (sensing, processing, communications, and mobility), and vulnerability.

These tradeoffs include the separation of the sensing and response functions. Standoff response devices may allow smaller sense devices to be deployed. Smaller sense devices should be easier to conceal within the environment. This tradeoff includes consideration of the area and time dimensions, including decision times involving the response device.

The advantages of the distributed ISR concepts, if realizable, enhance the DNS value propositions stated in section 3.2 as follows:

- *Creation of pervasive, persistent sensing sufficient for sustained awareness.* The capacity to employ a distributed sensor field to determine the optimal ISR location will reduce the time necessary to perform this function, thus allowing more collection time. A field that allows multiple sources and data collection at multiple locations provides a more pervasive ISR.

- *Extended capability reach via combat power distribution across manned and unmanned platforms.* The force multiplication and extended reach advantages are evident. Distributed ISR concepts also create options for risk reduction. Creation of a networked force to share awareness and to conduct distributed operations. A separation of the sense and respond functions should allow employment of greater numbers of small, pervasive, and covert sensors. The use of standoff response devices should allow an economy of force since response devices do not need to be paired with particular sensors. This use of distributed operation allows more effective use of force.

5. CONCLUSIONS

Complex distributed networked systems (DNS) are being developed for the purpose of enabling distributed networked forces (DNF) to conduct distributed networked operations (DNO). A DNF must have capabilities that have the potential to realize the advantages of the DNO and must also be employed so as to realize these advantages. A DNS must be developed with capabilities that have the potential to realize the advantages of a DNF and must also be employed so as to realize these advantages of a DNF. These advantages are the value propositions for the DNS.

The development of value propositions for various DNS concepts is more than an academic drill. The value propositions provide utility throughout the coevolution of the DNS technology and operational concepts, supported by experimentation.

Formation of a technology and operational concept should reflect the warfighters' vision and concept of how to conduct military operations. If the DNS concept developer carefully crafts the value propositions associated with his concept, the propositions can be used to confirm that the operational value of the concept is what the warfighter requires.

Articulation of the value propositions provides the framework from which to coevolve the technology and operational components of the concept. The developer must stay true to the value proposition or deliberately make changes based on the lessons learned.

Since the value propositions are articulated in operational terms, they become the foundation for operational experimentation. The value propositions can become the hypotheses for the experiment. Staying true to the value propositions precludes the degradation of the experiment into a technology demonstration. The technology may work, but, if the value proposition is not tested, the true military value will not be known.

6. REFERENCES

1. "National Security Strategy of the United States of America," President George W. Bush, The White House, Washington, DC, March 2006.

2. VADM John G. Morgan and RADM Charles W. Martoglio, "The 1,000-Ship Navy's Global Maritime Network," *U.S. Naval Institute Proceedings*, vol. 131/11/1,233, November 2005.

3. General M. W. Hagee, "A Concept for Distributed Operations," Department of the Navy, Headquarters U.S. Marine Corps, Washington, DC, 25 April 2005.

4. "Naval Operations Concept," Department of the Navy, Washington, DC, 2006.

5. Robert C. Manke and Raymond J. Christian, "Asymmetry in Maritime Access and Undersea Anti-Access/Area Denial Strategies," NUWC-NPT Technical Report 11,826, Naval Undersea Warfare Center, Newport, RI, 31 August 2007.

6. "Department of Defense Dictionary of Military and Associated Terms," Joint Force Publication 1-02, 1 March 2007, http://www.dtic.mil/doctrine/jel/new_pubs/JP1_02.pdf.

7. Sir B. H. Liddell Hart, *Strategy*, Praeger Publishers, New York, NY, 1972.

8. Mao Tse Tung, *On the Protracted War*, Foreign Languages Press, Peking, 1960.

9. Wayne P. Hughes Jr., *Fleet Tactics: Theory and Practice*, Naval Institute Press, Annapolis, MD, 1986.

10. Sir Julian S. Corbett, *Principles of Maritime Strategy*, Dover Publications, New York, NY, 2004.

11. General Rupert Smith, *The Utility of Force: The Art of War in the Modern World*, Alfred A. Knopf, New York, 2007.

12. General James T. Conway, Admiral Gary Roughead, and Admiral Thad W. Allen, "A Cooperative Strategy for 21st Century Seapower," Office of the Commandant, U.S. Marine Corps, Chief of Naval Operations, and Office of the Commandant, U.S. Coast Guard, Washington, DC, October 2007.

13. Richard W. Durham, "Operational Art in the Conduct of Naval Operations," School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, KS, 11 March 1998.

14. Raymond J. Christian, "Next-Generation Undersea Warfare and Undersea Distributed Networked Systems," NUWC-NPT Technical Report 11,790, Naval Undersea Warfare Center, Newport, RI, 31 January 2007.

15. Jeffrey R. Cares, Raymond J. Christian, and Robert C. Manke, "Fundamentals of Distributed, Networked Military Forces and the Engineering of Distributed Systems," NUWC-NPT Technical Report 11,366, Naval Undersea Warfare Center, Newport, RI, 9 May 2002.

16. "Quadrennial Defense Review Report," Office of the Secretary of Defense, Washington, DC, February 2006.

INITIAL DISTRIBUTION LIST

Addressee	No. of Copies
Office of the Secretary of Defense, Office of Net Assessment (A. Marshall)	1
Office of the Assistant Secretary of Defense (ASD-NNI – Deputy/CHENG)	1
Office of the Secretary of the Navy (Undersea Strategy Office – RADM (Ret.) W. Ellis, CAPT D. Norris)	2
Joint Forces Command (J9, JFCOM/MITRE – R. Richards)	2
Chief of Naval Operations (N00K, N3/N5 IW, N6F – K. Dufresne, N60, N61, N71, N6 Technical Director, N81 – T. Barber, N86F, N863, N864, N864A, N866, N87, N87B, N874, N874 – B. Raff, N875 – M. Orr, J. Zittel)	19
Commander, U.S. Fleet Forces Command (N8 Science Advisor)	1
Commander, Pacific Fleet (N00WAR – D. Yoshihara, RADM (Ret.) G. Gustavson)	2
Commander, Naval Network and Warfare Command (N8 – P. Jackson)	1
Commander, Center for Security Forces (N8 Science Advisor)	1
Strategic Studies Group (ADM (Ret.) J. Hogg, W. Glenney, R. Wilcox, A. Krulisch)	4
Naval Air Warfare Center, Aircraft Division (D. Backes)	1
Naval Air Warfare Center, Weapons Division (P. Yates)	1
Naval Mine and Anti-Submarine Warfare Command (00, J. Ferguson, D. Thigpen, S. Pelstring)	4
Naval Postgraduate School (RADM (Ret) R. Jones, J. Eagle, S. Gallup, W. Hughes, J. Kline, J. Rice)	6
Naval Research Laboratory (E. Franchi, F. Erskine)	2
Naval Sea Systems Command (PEO-C4I and Space – D. Bauman, PEO-IWS – Technical Director, PEO-IWS5 – C. Cannon, T. Carmean, PEO-SUB – Executive Director, SEA 05, SEA 05R, SEA 06, SEA 53, SEA 073, SEA 073 – W. Bankhead)	11
Naval Surface Warfare Center, Coastal Systems Center (D. Everhart, G. Kekalis, A. Sumey)	3
Naval Surface Warfare Center, Dahlgren Division (J. Moreland, NECE – A. Blankenship, SWE – M. Magdinec)	3
Naval Surface Warfare Center, Indian Head Division (NAE – C. Fawls)	1
Naval Undersea Warfare Center Division, Keyport (00, 01, 01A – G. Richards, 05 – J. Burwell, CAG – M. Tell, 41 – T. Lacey)	6
Naval War College (CNWS; NWC Library; WGD – W. Bundy; J. Fitzsimmons)	4
Naval Warfare Development Command, Newport (N00)	1
Office of Naval Research (ONR 03R, ONR 03T, ONR 31, ONR 32, ONR 33)	5
Space and Naval Warfare Systems Center, San Diego (D. Endicott, E. Hendricks, G. Galdorisi, M. Gmitruk, S. Stewart)	5
Defense Advanced Research Projects Agency (STO – D. Honey, B. Pierce, L. Stotts, K. Latt, E. Carapezza; TTO – S. Welby, S. Walker; IXO – R. Tenny, M. Davis, A. Moshvegh)	10
Alidade Inc. (B. Braswell, J. Cares, J. Dickman)	3
Center for Naval Analyses (H. Spivack)	1
Institute for Defense Analyses (J. Hanley)	1
Johns Hopkins University, Applied Physics Laboratory (VADM (Ret.) J. Fitzgerald, J. Benedict, L. Blodgett, K. Britzenhofe, L. Green, R. Henrick, E. Holmboe, R. Mitnick, D. Tyler)	9
Lockheed Martin Corporation, Orincon Division (H. Cox)	1
Massachusetts Institute of Technology (A. Baggeroer)	1
Massachusetts Institute of Technology Center for International Studies (Security Studies Program – O. Cote)	1
University of Texas at Austin, Applied Research Laboratories (C. Penrod)	1
Defense Technical Information Center	2